International Journal of Innovation Scientific Research and Review
Vol. 04, Issue, 08, pp.3157-3165, August 2022
Available online at http://www.journalijisr.com
SJIF Impact Factor 4.95

IJISRR

ISSN: 2582-6131

Research Article

GIVEN THE SEC'S 2022 PROPOSED CYBER RULE AMENDMENTS,IS THE DOD'S CMMC FRAMEWORK A VIABLE CYBER FRAMEWORK?

*** Donald L. Buresh, Ph.D., Esq.**

Received 08th June 2022; Accepted 09th July 2022; Published online 20th August 2022

ABSTRACT

This essay aims to discuss the Security and Exchange Commission (SEC) proposed cyber rule changes, and their effect on cyber security risk management frameworks, particularly the Cyber security Maturity Model Certification (CMMC) framework, currently advocated by the Department of Defence. The issues surrounding the SEC proposed rule changes are discussed, pointing out their benefits and limitations. The CMMC framework is then described, observing that for CMMC 2.0 Level 2 and Level 3 compliance, an entity must be NIST SP 800-171 and NIST SP 800-172 compliant, respectively. Three other frameworks are discussed, including the NIST Cyber security Framework, the ISO/IEC 27001 framework, and the HITRUST Cyber Security Framework and its current variations. The article points out that only HITRUST i1 and HITRUST r2 are likely CMMC 2.0 compliant. The paper concludes by noting that when a firm is faced with the SEC proposed cyber rule changes and CMMC 2.0, how a company behaves is dependent on its current cyber security situation and whether it wishes to become or remain a defence contractor or sub-contractor. Even so, by adhering to some cyber security framework, a firm is likely evolving into an organization that treats cyber security as a normal business operation, much like accounting, finance, or marketing.

Keywords: Cyber security Maturity Model Certification, HITRUST Cyber Security Framework, ISO/IEC 27001, NIST Cyber security Framework, NIST SP 800-171, NIST SP 800-172, SEC Proposed Cyber Rule Changes.

INTRODUCTION

This essay aims to discuss whether the Security and Exchange Commission's (SEC) 20202 proposed cyber amendments are viable in the light of the Department of Defense's (DoD) advocacy and support of the Cyber security Maturity Model Certification (CMMC). The paper first outlines the SEC's proposed cyber rule amendments and explains the challenges of the proposed rule changes. The article then describes the costs and benefits of the proposed rule changes, followed by a brief examination of the intersection between the proposed rule changes and various state laws.

The paper then changes course by evaluating CMMC and other well-known cyber security frameworks. The essay points out some of the reasons why other cyber frameworks are not equivalent to NIST SP 800-171 or NIST SP 800-172, two frameworks that are currently an integral part of CMMC. The article evaluates under what circumstances a firm would or would not pursue CMMC certification. It is important to remember that CMMC certification may be an expensive activity and not necessarily suited for all companies. The paper concludes by remarking that the SEC proposed rule changes and CMMC may well be the impetus to bring cyber security into the mainstream, where geekiness is abandoned, leaving cyber security in a similar position as Generally Accepted Accounting Principles (GAAP) accounting, essential business behavior.

The 2022 Proposed Cyber security Rules

In February 2022, the SEC released the proposed cyber rules for registered investment advisers and investment funds.[1] With its intention turned to public companies, on March 9, 2022, the SEC proposed amendments to its rules to augment and standardize corporate disclosures regarding cyber security risk management, strategy, governance, and incident reporting.[2]The proposed amendment aimed to require current reporting on material cyber security incidents and updates on previous cyber security incidents to provide notification to investors about material cyber security incidents.[3] The proposed amendments were published on the SEC and Federal Register (FR) websites. The comment period was for 60 days from the publication on the SEC website and 30 days from the release by the FR, whichever is longer.[4]

The SEC stated that the Form 8-K, a report of unscheduled material events or corporate changes, would be the primary vehicle for reporting a cyber security incident within four business days after determining that material incident occurred.[5] The information in Form 8-K should consist of:

- When the incident was discovered and whether it is an ongoing event;
- A concise description of the nature and scope of the event;
- Whether data was stolen, altered, accessed, or used for any unauthorized purpose;
- The outcome of the incident on the entity's operations; and
- Whether the incident has been remedied or is being remedied.[6]

The effect of the proposed rule change was that it would put an extra burden on firms to understand the nature of a cyber breach and its materiality. This effect is significant as ransom ware continues to permeate the business climate, creating financial costs, fines, penalties and litigation costs, business continuity risks, and extensive

[1]Paul Ferillo, *Proposed SEC Cyber Rules: A Game Changer for Public Companies*, HARVARD LAW SCHOOL FORUM ON CORPORATEGOVERNANCE (Apr. 11, 2022), *available at*https://corpgov.law.harvard.edu/2022/04/11/proposed-sec-cyber-rules-a-game-changer-for-public-companies/.

[2]Press Release, SECURITIES AND EXCHANGE COMMISSION, *SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*(Mar. 9, 2022), *available at*https://www.sec.gov/news/press-release/2022-39.

[3]*Id.*

[4]*Id.*

[5]Paul Ferillo, *supra*, note 1.

[6]*Id.*

economic exposure.[7] The critical aspects of the proposed rule changes include:

- Reporting material cyber security incidents within four days;
- Updates of previously reported incidents;
- Required disclosure of cyber security risk management and strategy;
- Required disclosures regarding cyber security governance;
- Required disclosures about cyber security expertise on the board of directors;
- Foreign private issuers are required to supply cyber security disclosures via Forms 6-K and 20-F; and
- Reporting must be present in Inline extensible Business Reporting Language (XBRL) in machine-readable and human-readable formats.[8]

Because the SEC proposed rules would amend Item 407 of Regulation S-K regarding corporate governance requiring disclosure of cyber security expertise on the board of directors, it is similar to the current director disclosure requirement that a director reveals financial expertise on a company's audit committee.[9] The disclosure would involve whether:

- A director has prior work experience in cyber security;
- A director possesses a certification or a degree in cyber security; and
- A director has knowledge, skills, or other backgrounds in cyber security.[10]

The message is clear. Cyber security is a topic that firms must vigorously address both on their boards and in the halls of their management.

The Challenges that the Proposed Amendments Pose

There are various challenges that the proposed amendments present. First, the four-day incident reporting rule is an issue because it may not be possible to provide the desired information in the allotted timeframe. The company may not have the technical expertise to accurately diagnose a cyber incident under the proposed time constraint. It is also likely that third-party expertise may need additional time to evaluate an incident to avoid reporting false positives or negatives. Second, providing updates on previous cyber incidents is arduous, as it is unclear how far back in time the company should go in its reporting. If public companies are required to report previous cyber incidents, a plethora of 8-Ks could be released, which could seriously negatively affect investor confidence.

Third, by disclosing a company's cyber security risk management and strategy, an entity may be opening itself up for additional attacks. Cybercriminals could use this information to craft further cyber-attacks by searching for vulnerabilities in a company's defenses. Fourth, disclosure of corporate governance could also result in added attacks for the same reason. Fifth, it may not be easy to find directors with cyber security expertise. Directors are typically selected based on their ability to oversee a firm, not predicated on their cyber security expertise. Cyber security is a relatively new field, and individuals with such expertise may be unqualified to sit on a board of directors. Sixth, foreign private issuers may not desire to provide cyber security disclosures because of their distance from American markets. Finally, the reporting requirement that statements be presented in XBRL in both machine-readable and human-readable formats could be an issue if there is a lack of technical expertise in the labor market, causing the hourly labor rate to increase dramatically. This would likely be a short-term shortage because the information technology market would probably race to satisfy the demand.

Proposed Rule Changes and Cyber security Risk Management

In the long run, the proposed rules will likely support cyber security risk management because they would force companies to adopt a cyber risk management framework to protect the company from attacks and to ensure that if a cyber-attack occurs, the reporting mechanisms (including software) will reveal the nature of the attack promptly. The supply chain implications of the proposed rules are evident because the proposed rule changes would thrust cyber security risk management frameworks into the corporate mainstream. Cyber security frameworks would become as standard in the corporate environment as GAAP accounting reporting. Cyber security would no longer be an esoteric subject known only to the shamans of information technology. In particular, with the proposed rule changes, cyber security would likely become a conventional corporate activity among its department and employees. Cyber security would rapidly mature, where its initiates would no longer dress in geeky outfits but adopt the corporate lifestyle's tone, manner, and dress.

Benefits and Costs of the Rules Amendments

In determining whether the proposed rule changes' potential benefits outweigh the challenges they create, the response must address whether the benefits and costs occur in the short-run or the long-run. In the short run, some of the expenses are immediate. For example, reporting previous cyber incidents may be burdensome, assuming that the new information in Form 8-K was not previously provided. Other short-run costs include installing the reporting mechanisms on short notice. A cyber-attack could happen before a firm was adequately prepared to report on it. This scenario could occur if a firm implemented a cyber risk management framework and cybercriminals decided to hack the company's system. The result would likely be chaotic, where employees were scrambling to comply with the proposed rules without possessing sufficient information about an attack. The negative goodwill incurred could be substantial.

The proposed rule changes benefits would probably manifest over a more extended period. It takes time and effort to implement a cyber security risk management framework. The period could range from several months to over a year. The good news is that once a risk management framework was in place, the reporting delays would likely be minimal. The cyber security mechanisms to detect, mitigate, and counter a cyber-attack would become a normal operating procedure, where employees and consultants alike would know instinctively what to do, where to do it, when, and how to do it. The financial benefits to a firm could be substantial. No longer would companies be struggling to address a cyber-attack. Employees and consultants would react with the assurance that their efforts would resolve the issue.

Proposed Rules Changes and Existing State Laws

All 50 states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have laws requiring private businesses and most states, including governmental agencies, to notify individuals of

[7] *Id.*
[8] *Sidley Staff, NewlyProposed SEC Cybersecurity Risk Management and Governance Rules and Amendments for Public Companies, SIDLEY AUSTIN LLP (Mar. 11, 2022), available athttps://www.sidley.com/en/insights/newsupdates/2022/03/newly-proposed-sec-cybersecurity-risk-management-and-governance-rules.*
[9] *Paul Ferillo, supra, note 1.*
[10] *Id.*

personally identifiable information security breaches.[11] State cyber breach laws possess provisions regarding who must comply, such as businesses, data or information brokers, or government agencies.[12]According to the National Council of State Legislatures (NCSL), different laws apply to individuals and business versus government entities exist.[13]Each state may have a different definition of what constitutes personal information. Specific personal information may include an individual's name, social security number (SSN), driver's license or state ID, or account numbers.[14] There are also likely different definitions of what constitutes a breach or unauthorized data acquisition, the timing or method of notice, or who must be notified.[15] Finally, state laws may have exemptions for encrypted information.[16]Each state's laws must be examined to determine whether there is an intersection between a given state's breach of law and the SEC's proposed rule changes. It is a detailed task that demands substantial effort.

Cyber security Maturity Model Certification

On November 4, 2021, the Department of Defense announced the strategic direction of the CMMC program.[17] This enhanced version of CMMC (CMMC 2.0) desired to safeguard sensitive information while:

- Simplifying the CMMC standard by supplying additional information on cyber security regulatory policy and contracting requirements;
- Concentrating innovative cyber security standards and third-party assessments requirements on companies that support high-priority programs;
- Enlarging the oversight of professional cyber security ethical standards.[18]

It was projected that these enhancements will:

- Enhance company accountability while minimizing compliance barriers;
- Create a collaborative cyber security culture;
- Encourage the public trust while alleviating the execution burden.[19]

The point of the CMMC standard is to assure that DoD contractors and sub-contractors are compliant with DoD standards.

The features of the CMMC program include (1) a tiered model that demands that companies that possess national security information employ cyber security standards at advanced levels, depending on the criticality of the information; (2) an assessment requirement that permits the DoD to verify the cyber security standards implemented by a contractor or sub-contractor; and (3) a requirement that DoD contractors that deal with controlled unclassified information (CIU) achieve a specified CMMC level before being awarded a contract.[20]

The original version of CMMC (CMMC 1.0) was announced in September 2020. When the DoD unveiled CMMC, the new standard provided a new compliance cyber security framework for DoD acquisitions.[21] The framework is similar to the management maturity models first devised by the Software Engineering Institute (SEI) at Carnegie-Mellon University (CMU).[222324] CMMC 1.0 contained five levels, ranging from basic to advanced, and the essential features of the standard are contained in Table 1.[25]

Table 1. Features of the CMMC 1.0 Model.

Level	Practices	Processes	Assessments
Level 5: Advanced	171	5	Third Party
Level 4: Proactive	156	4	None
Level 3: Good	130	3	Third Party
Level 2: Intermediate	72	2	None
Level 1: Basic	17	None	Third Party

In March 2021, the DoD initiated an internal review of CMMC 1.0 and received over 850 public comments.[26] The response indicated that CMMC 1.0 was overly complicated for contractors and subcontractors to implement. In November 2021, the DoD updated CMMC 1.0, coming out with CMMC 2.0, a simpler version. Table 2 highlights the main features of CMMC 2.0.[27]

Table 2. Features of the CMMC 2.0 Model.

Level	Practices	Assessments	Comments
Level 3: Expert	145	Triennial government-led assessments.	Practices based on NIST SP 800-172
Level 2: Advanced	110	Triennial third-party assessments for critical national security information. Annual self-assessments for selected programs.	Practices based on NIST SP 800-171
Level 1: Foundational	17	Annual self-assessment.	N/A

The advantages of CMMC 2.0 over CMMC 1.0 are evident. CMMC 2.0 has been streamlined, going from five to three compliance levels, where CMMC 2.0 applies the National Institute of Standards and Technology (NIST) cyber security standards.[28] CMMC 2.0 permits any company at Level 1 (Foundational) and a subset of Level 2 (Advanced) firms to show compliance via self-assessment.[29]The new CMMC standard increases oversight of professional and ethical standards of third-party assessors.[30]CMMC 2.0 has reduced assessment costs because organizations can make Plans of Actions & Milestones (POA&M) to attain certification under limited

[11]NCSL Staff, *Security Breach Notification Laws*, NATIONAL CONFERENCE OF STATE LEGISLATURES (Jan. 17, 2022), *available at*https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
[12]*Id.*
[13]*Id.*
[14]*Id.*
[15]*Id.*
[16]*Id.*
[17] DoD Staff, *Strategic Direction for CybersecurityMaturity Model Certification (CMMC) Program*, UNITED STATES DEPARTMENT OF DEFENSE (Nov. 4, 2021), *available at*https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-model-certification-cmmc-program/.
[18]*Id.*
[19]*Id.*
[20] DoD Staff, *About CMMC*, OFFICE OF THE UNDER SECRETARY OF DEFENSE: ACQUISITION AND SUSTAINMENT (n.d.), *available at*https://www.acq.osd.mil/cmmc/about-us.html.
[21]*Id.*
[22]*Id.*
[23]MARK C. PAULK, CHARLES V. WEBER, BILL CURTIS, & MARY BETH CHRISSIS, THE CAPABILITYMODEL: GUIDELINES FOR IMPROVING THE SOFTWARE PROCESS, CARNEGIE-MELLON UNIVERSITY(Addison-Wesley Publishers 1995).
[24]WATTS HUMPHREY, MANAGING THE SOFTWARE PROCESS (Addison-Wesley Publishers 1989).
[25]DoD Staff, *supra*, note 4.
[26]*Id.*
[27]*Id.*
[28]*Id.*
[29]*Id.*
[30]*Id.*

circumstances.[31] Finally, under specific conditions, waivers of CMMC requirements may be obtained.[32]

According to the DoD, the department intends to permit firms to accept contract awards with a POA&M to implement CMMC requirements.[33] The DoD intends to stipulate a baseline number of requirements that should be attained before a contract is awarded and then permit the remaining requirements to be addressed in the POA&M with a well-defined timeline.[34] The DoD reserves the right to identify a small collection of CMMC certification requirements that cannot be part of a POA&M.[35]

The DoD has intended to create a limited waiver process to exclude CMMC requirements for some mission-critical requirements. The department envisions waiver requests will need senior DoD leadership approval and will have a limited duration. The specifics of the waiver process have yet to be determined but will be addressed in the rule-making process.[36]

According to Pomerleau, the DoD is projecting that it will implement CMMC in May 2023.[37] The department wants to prod the hundreds of thousands of defense contractors to ensure that their networks and CUI are protected. At the Potomac Officer Club, Stacy Bostjanick, the CMMC policy director, stated that the DoD hopes that by March 2023, the federal rule-makers will give the DoD an interim rule.[38] Bostjanick also said that the federal rule-makers might not see the urgency of an interim rule requiring the DoD to implement CMMC until the department goes through the final rule process.[39] However, if an interim rule is granted, the CMMC program will proceed to a 60-day public comment period.[40] During the 60-day comment period, the DoD will be allowed to implement CMMC in its contracts and acquisitions by May 2023.[41]

Bostjanick pointed out that the DoD will be phasing in CMMC to ensure the entire DoD cyber security ecosystem, including assessor and instructor certification organizations, assessors, the Defense Industrial Base Cyber security Assessment Center (DIB-CAC), and other entities, are prepared to address contractor and subcontractor certification needs.[42] Bostjanick said that for entities that handle non-prioritized CUI, a self-assessment that satisfies NIST SP 800-171 should be sufficient.[43] Because many companies bid on multiple DoD contracts, such an organization will probably be required to undergo a third-party assessment. Bostjanick observed that future DoD contracts would state whether the procurement includes prioritized CUI, non-prioritized CUI, or Level 3 CUI.[44] Currently, under CMMC 2.0, Level 3 demands an assessment from the DIB-CAC.[45] Although rough definitions are in flux, the department is assembling an acquisition guide for program managers and contracting officers to help them understand what constitutes prioritized and non-prioritized CUI.[46]

Ransom ware Attacks and the CMMC

The DoD wants its contractors and subcontractors to implement CMMC to avoid ransom ware issues. Ransom ware is "malware that prevents or limits users from accessing their system, either by locking the system's screen or locking the users' files until a ransom is paid."[47]Crypto-ransom ware is a modern form of ransom ware, where a user's files are encrypted, and the cybercriminal forces users to pay the ransom, typically in crypto-currency, iTunes, and Amazon gift cards, to avoid detection to obtain a decryption key.[48]Ransom ware prices depend on the ransom ware software being employed.

Ransom ware may be downloaded onto systems by users that visit malicious or compromised websites. It can also be put on a system as a payload that is deposited by malware or appears as an attachment from an unsolicited email site.[49] For example, ransom ware can be dropped on a system via an SQL injection, where an SQL statement is entered instead of valid data, much like what happened in the initial phases of the Solar Winds breach.[50]

From the federal government's perspective, ransom ware is particularly troublesome because a cybercriminal may likely be from Russia.[51]Ransom ware cases were initially observed in Russia between 2005 and 2006.[52] For example, in 2006, Trend Micro published a report about ransom ware that zipped specific files before overwriting the original files, leaving only password-protected files on a system. The ransom ware (TROJ_CRYZIP.A) also generated a text file that served as a ransom note, stating that users could retrieve their files for a $300.00 payment.[53] It should be remembered that because of its profitability, the malware quickly migrated to Europe and North America.[54] Even so, given the current economic and political animosity between the United States and Russia and the risk that federal government data on a contractor' system may be taken even if the ransom is paid, ransom ware is one of several reasons why a robust cyber security risk management framework is essential in this Cold War 2.0 era.

The NIST SP 800-171 Standard

The NIST SP 800-171 standard, first published in 2015, is a required security standard for non-federal organizations that possess CUI on their networks.[55] Revision 2 is the latest version of the standard, and it was released in February 2020.[56] The standard only applies to that part of a contractor's network where CUI resides. The purpose of NIST SP 800-171 is to harden the security of the federal supply chain by creating a unified cyber security baseline for contractors and sub-contractors with access to CUI.[57]

[31] *Id.*
[32] *Id.*
[33] *DoD Staff, CMMC Implementation, OFFICE OF THE UNDER SECRETARY OF DEFENSE: ACQUISITION AND SUSTAINMENT (n.d.), available at https://www.acq.osd.mil/cmmc/implementation.html#impHero.*
[34] *Id.*
[35] *Id.*
[36] *Id.*
[37] *Mark Pomerleau, Pentagon Updates Timeline for CMMC Cybersecurity Initiative, FEDSCOOP (May 18, 2022) available athttps://www.fedscoop.com/pentagon-updates-timeline-for-cmmc-cybersecurity-initiative/.*
[38] *Id.*
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Trend Micro Staff, Ransomware, TREND MICRO (2022), available athttps://www.trendmicro.com/vinfo/us/security/definition/ransomware.*
[48] *Id.*
[49] *Id.*
[50] *Kingthorin, SQL Injection, OWASP (n.d.), available athttps://owasp.org/www-community/attacks/SQL_Injection.*
[51] *Trend Micro Staff, supra, note 47.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Titania Staff, What Is NIST SO 800-171? How to Stay Compliant in 2021, TITANIA (2022), available athttps://www.titania.com/resources/guides/nist-800-171/,*
[56] *Id.*
[57] *Id.*

The NIST SP 800-171 standard has 14 families divided into 110 security requirements.[58] The 14 requirement families and requirements are listed in Table 3.[59]

Table 3. NIST SP 800-171 Requirement Families and Requirements

Access Control (22 requirements)	Media Protection (9 requirements)
Awareness and Training (3 requirements)	Personal Security (2 requirements)
Audit and Accountability (9 requirements)	Physical Protection (6 requirements)
Configuration Management (9 requirements)	Risk Assessment (3 requirements)
Identification and Authentication (11 requirements)	Security Assessment (4 requirements)
Incident Response (3 requirements)	System and Communication Protection (16 requirements)
Maintenance (6 requirements	System and information (7 requirements)

There is currently no certification body or official auditing mechanism to establish where a contractor or sub-contractor is adhering to the NIST SP 800-171 standard. Organizations must self-assess or hire a third party to verify compliance.[60] Defense contractors employ a points-based system to show compliance. The process comprises a self-assessment against the 110 requirements in NIST SP 800-171. Entities are given a point for every implemented requirement, where the maximum score is 110, but where weighted penalty points are subtracted for each unimplemented or partially implemented requirement.[61] Defense contractors must also submit a System Security Plan (SSP) to demonstrate NIST SP 800-171 compliance. Any requirements not achieved by a DoD contractor should be stated in its POA&M with critical dates and timelines for achieving full compliance and before a contract begins.[62]The POA&M can be updated as the entity that deals with non-compliance requirements.

The NIST SP 800-172 Standard

NIST SP 800-172, published in February 2021, is a companion document to NIST SP 800-171, and its purpose was to reinforce an entity's resistance against advanced cyber security risks such as Advanced Persistent Threats (APT).[63] An APT is defined in NIST SP 800-172 as "an adversary that has the resources and expertise to attack systems through different attack vectors."[64]Attack channels may include cyber threats, physical system access, or deception campaigns.[65]A nation-state could sponsor an APT attack. The attack would likely be complex compared to an entity's defenses and occur over an extended period. An APT may not be promptly detected because it aims to gain system access for future attacks or data breaches.[66]NIST SP 800-172 establishes an enhanced selection of security controls when CUI is associated with critical systems and programs. NIST SP 800-172 consists of 35 enhanced requirements that transcend the 110 requirements listed by NIST SP 800-171.[67] The aim is to strengthen the federal government against APTs and other security threats to ensure that at-risk data is as secure as possible on non-federal systems.[68] The enhanced requirements are associated with the 14 requirements families and appear in Table 4.

Table 4. NIST SP 800-172 Requirement Families and Enhanced Requirements

Access Control (3enhanced requirements)	Media Protection (no enhanced requirements)
Awareness and Training (2enhanced requirements)	Personal Security (2 enhanced requirements)
Audit and Accountability (no enhanced requirements)	Physical Protection (no enhanced requirements)
Configuration Management (3 enhanced requirements)	Risk Assessment (7 enhanced requirements)
Identification and Authentication (3 enhanced requirements)	Security Assessment (1 enhanced requirement)
Incident Response (2 enhanced requirements)	System and Communication Protection (5 enhanced requirements)
Maintenance (no enhanced requirements	System and information (7 requirements)

If a firm decides to become NIST SP 800-172 compliant, there are 145 requirements. Table 5 lists the total number of NIST SP 800-172 compliant requirements.

Table 5. NIST SP 800 - 172Requirement Families and Total Requirements

Access Control (25total requirements)	Media Protection (9 total requirements)
Awareness and Training (5total requirements)	Personal Security (4total requirements)
Audit and Accountability (9 total requirements)	Physical Protection (6 total requirements)
Configuration Management (12total requirements)	Risk Assessment (10total requirements)
Identification and Authentication (14 total requirements)	Security Assessment (5total requirements)
Incident Response (5 total requirements)	System and Communication Protection (21total requirements)
Maintenance (6 total requirements	System and information (14 total requirements)

The three elements of the NIST SP 800-172 enhanced protection program are (1) a penetration-resistant architecture, (2) damaging-limiting outcomes, and (3) cyber resiliency survivability.[69] The enhanced requirements are balanced against the three elements of the protection strategy, thereby lowering the risk of a successful cyber-attack.

Other Cyber security Frameworks

In CMMC 2.0, depending on whether an organization is at Level 2 or Level 3 compliance, an entity must be NIST SP 800-171 or NIST SP 800-172 compliant. However, what if a company complies with another standard not part of the NIST family of standards? What if the standard is equivalent to either NIST SP 800-171 or NIST SP 800-172? This section of the paper will discuss the NIST Cyber security Framework (CF), the ISO/IEC 27001 framework, the HITRUST Cyber Security Framework (CSF).

[58] *Id.*
[59] *Id.*
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] Titania Staff, *What Is NIST 800-172?Requirement for Protecting CUI*, Titania (2022), available at https://www.titania.com/resources/guides/what-is-nist-sp-800-172--requirements-for-protecting-cui/.
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*

NIST Cyber security Framework

The NIST Cyber security Framework (CF) is a standard for protecting critical infrastructure, such as roads, bridges, airports, etc.[70] CF deals with business drivers that influence cyber security activities that affect an entity's risk management processes.[71] The three parts of CF are the Framework Core, the Implementation Tiers, and the Framework Profiles.[72]The Framework Core is a collection of activities, outcomes, and informative references generic to industry sectors and critical infrastructure.[73] Implementation Tiers help a corporation view and understand the features of their approach in managing their cyber security risk, thereby prioritizing their cyber security objectives.[74] The Framework Profiles assist an organization in aligning and ordering its cyber security activities with its business mission requirements, risk tolerances, and resources.[75]

The CF functions are identify, protect, detect, respond, and recover.[76] Each function contains a collection of categories. Table 6 lists each category's functions, associated categories, and ID.

Table 6. NIST Cyber security Framework Categories

Function	Category
Identity	Asset management
	Business environment
	Governance
	Risk Assessment
	Risk management strategy
	Supply chain risk management
Protect	Identity management and access control
	Awareness and training
	Data security
	Information protection processes and procedures
	Maintenance
	Protective technology
Detect	Anomalies and events
	Security continuous monitoring
	Detection processes
Respond	Response planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery planning
	Improvements
	Communications

On its face, CF appears to be an extensive cyber security framework that could be equivalent to NIST SP 800-171 or NIST SP 800-172. However, when mapped carefully to either one of these frameworks, CF comes up wanting.[77]CF is not equivalent to NIST SP 800-171 because there are requirements in NIST SP 800-171 that do not have an equivalent requirement in CF. Also, CF is not equivalent to NIST SP 800-172 because it has more requirements than NIST SP 800-171. The result is that any organization that is CF compliant is likely not NIST SP 800-171 compliant and thus unable to satisfy CMMC 2.0 Level 2. Even so, the entity may be CMMC 2.0 Level 1 compliant, depending on the extent of the CF implementation.

ISO/IEC 27001 Security Framework

ISO/IEC 27001 is an international standard regarding information security management. In 2005, the International Organization for Standardization (ISO) and the International Electro technical Commission (IEC) published the original standard jointly.[78] The standard was revised in 2013.[79] The standard describes the requirements to establish, implement, maintain, and continually improve an information management system by making information assets secure.[80] There was a European update of the standard that was published in 2017.[81] After completing an audit, an organization can be certified by the ISO.

ISO/IEC 27001 certification[82] is a three-step process defined by ISO/IEC 17021[83] and ISO/IEC 27006[84] standards. The process includes:

- ***Stage 1*** – A preliminary review of an organization's information security management system (ISMS) that checks for critical security documentation, Statement of Applicability (SoA), and the Risk Treatment Plan (RTP);
- ***Stage 2*** – A formal compliance audit compares the entity's ISMS against the ISO/IEC 27001 standard. The audit seeks confirmation that the ISMS is appropriately designed, implemented, and in operation. ISO/IEC Lead Auditors usually conduct the audit. Once a company passes this stage, it is fully ISO/IEC 27001 certified.
- ***Ongoing***– This stage concerns follow-up reviews to ensure that the organization complies with the standard by employing periodic reassessment audits at least annually.

ISO/IEC 27001 consists of ten clauses and a long annex. Table 7 summarizes the content for the 14 relevant annexes.[85]

[70]*Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Apr. 6, 2018), *available at*https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf.
[71]*Id.*
[72]*Id.*
[73]*Id.*
[74]*Id.*
[75]*Id.*
[76] NIST Staff, *An Introduction to the Components of the Framework*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) (May 24, 2021), *available at* https://www.nist.gov/cyberframework/online-learning/components-framework.
[77]*CSF to SP 800-171 Mapping Disclaimer*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (n.d.) *available at* https://csrc.nist.gov/CSRC/media/Publications/sp/800-171/rev-2/final/documents/csf-v1-0-to-sp800-171rev2-mapping.xlsx.
[78]*ISO/IEC 27001 International Information Security Standard Published*, BRITISH STANDARDS INSTITUTION (Nov. 2, 2005), *available at*https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2005/11/ISOIEC-27001-International-Information-Security-Standard-published/.
[79] Katie Bird, *New Version of ISO/IEC 27001 to Better Tackle IT Security Risks*, INTERNATIONAL STANDARDS ORGANIZATION (Oct. 2013), *available at*https://www.iso.org/news/2013/08/Ref1767.html.
[80]*ISO/IEC 27001:2013 Information technology – Security Techniques – Information Security Management Systems – Requirements*, INTERNATIONAL STANDARDS ORGANIZATION (Aug. 14, 2013), *available at*https://www.iso.org/standard/54534.html,
[81]BS EN ISO/IEC 27001:2017 – What Has Changed?, BRITISH STANDARDS INSTITUTION (n.d.), *available at*https://www.bsigroup.com/en-GB/iso-27001-information-security/BS-EN-ISO-IEC-27001-2017/.
[82]*The ISO27001 Certification Process*, THE ISO 27000 DIRECTORY (2007), available at http://www.27000.org/ismsprocess.htm.
[83]*ISO/IEC TS 17021-2:2012 ConformityAssessment – Requirements for Bodies Providing Audit and Certification of Management Systems – Part 2: CompetenceRequirements for Auditing and Certification of Environmental Management Systems*, INTERNATIONAL STANDARDS ORGANIZATION (Revised 2016), *available at*https://www.iso.org/standard/59884.html,
[84] ISO/IEC 27006:2011 Information Technology – Security Techniques – Requirements for Bodies Providing Audit and Certification of Information Security Management Systems, INTERNATIONAL STANDARDS ORGANIZATION (Revised 2015), *available at*https://www.iso.org/standard/59144.html.
[85] Luke Irwin, *ISO 27001 Annex A Controls Explained*, IT GOVERNANCE (Jul. 27, 2020), *available at*https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained.

Table 7. ISO/IEC 27001 Annexes

Annex	Description
Annex A.5	Information security policies (2 controls)
Annex A.6	Organization of information security (7 controls)
Annex A.7	Human resource security (6 controls)
Annex A.8	Asset management (10 controls)
Annex A.9	Access control (14 controls)
Annex A.10	Cryptography (2 controls)
Annex A.11	Physical and environmental security (15 controls)
Annex A.12	Operations security procedures and responsibilities (14 controls)
Annex A.13	Communications security, including information network management and information transfer (7 controls)
Annex A.14	System acquisition, development, and maintenance (13 controls)
Annex A.15	Supplier relationships and supplier service delivery management (5 controls)
Annex A.16	Information security incident management and improvement(7 controls)
Annex A.17	Information security aspects of business continuity management dealing with continuity and redundancy(4 controls)
Annex A.18	Compliance with legal and contractual requirements (8 controls)

Again, based on the apparent complexity of the ISO/IEC27001 standard, one might be led to believe that the standard is equivalent to CMMC 2.0. However, looks can be deceiving. According to Maytech, ISO/IEC 27001 and NIST SP 8000-171 cover the same security areas, but one does not precisely map to the other.[86] A detailed mapping process must be examined to reveal this fact. Appendix D of the NIST 800-171 (Revision 1) manual attempts to map each requirement statement in NIST SP 800-171 against the equivalent control in ISO 27001.[87] The issue is that some NIST SP 80-0-171 requirements have no direct mapping or equivalent ISO/IEC 27001 control.[88] This means that ISO/IEC 27001 does not entirely satisfy the NIST SP 800-171 standard. Thus, at most, an ISO/IEC 27001 compliant organization would be CMMC 2.0 Level 1 compliant.

HITRUST Cyber Security Frameworks

The HITRUST Common Security Framework (CSF) is a common security and privacy framework that delivers structure, transparency, guidance, and cross-references to entities that must be certain of their data protection compliance and other organizations that interact with it.[89] The core structure of the CSF is predicated on ISO/IEC 27001 and 27002.[90] However, it includes 40 additional security and privacy-related regulations, standards, and frameworks, ensuring comprehensive and prescriptive coverage.[91]

HITRUST declared that adopting common security and privacy framework is "necessary, but not sufficient to ensure coverage and compliance confidence."[92] Hi Trust offers the HITRUST CSF Assurance Program and MyCSF.[93] The HITRUST CSF Assurance Program is a simplified compliance assessment reporting tool that uses a common approach to manage security assessments, creates efficiencies, and contains costs associated with various assurance requirements.[94]MyCSF is a software as a service (SaaS) information risk management platform that provides an efficient solution for assessing, managing, and reporting information risk and compliance.[95]

The control categories in the CSF include control objectives and control specifications that leverage the primary categories from the ISO/IEC framework, as well as specific categories for an information management security program and risk management practices that safeguard organizational, regulatory, and system controls are correctly specified and implemented.[96] The CSF possesses 14 control categories that consist of 49 control objectives and 156 control specifications. The control objectives are listed first in parentheses, followed by the control specifications. The key components are listed in Table 8.[97]

Table 8. Key Components of the HITRUST Cyber Security Framework

Information Management Security Program (1,1)	Asset Management (2, 5)
Access Control (7, 25)	Physical and Environmental Security (2, 13)
Human Resources Security (4, 9)	Communications and Operations Management (2, 5)
Risk Management (1, 4)	Information Systems Acquisition, Development, and Maintenance (6, 13)
Security Policy (1, 2)	Information Incident Security Management (2, 5)
Organization for Information Security (2, 11)	Business Continuity Management (1,5)
Compliance (3, 10)	Privacy Practices (7, 21)

The order of the control categories is not critical. The architecture of a control category is outlined in Table 9.[98]

HITRUST recently announced the new HITRUST Basic, Current-state (HITRUST bC) Assessment and the HITRUST Implemented, 1-year (HITRUST i1) Validated Assessment with Certification.[99] These new HITRUST options are flexible and quickly result in HITRUST certification while reducing costs and effort. HITRUST also rebranded HITRUST CSF Validated certification, now calling it the HITRUST Risk-based, 2-year (HITRUST r2) Certification.[100]

Table 9. The Architecture of a HITRUST CSF Control Category

Control Category	Comment
Control Objective	A statement of the desired result.
Control Reference	The control number and title.
Control Specification	Policies, procedures, guidelines, practices, or organizational structures that are managerial, operational, technical, or legal
Risk Factor Type	Predefined organizational, regulatory, or system risk factors that increase the risk to an entity.
Topics	Keywords indicating relevant categories affiliated with the control reference.
Implementation Requirements	Detailed information to support the implementation of a control.

[86] Maytech Staff, *NIST 800-171 Compliance*, MAYTECH GLOBAL DATA TRANSFER (2022), *available at*https://www.maytech.net/features/nist-800-171-compliance#:~:text=ISO%2027001%20and%20NIST%20800,standard%20you%20are%20operating%20under.

[87]Ron Ross, Patrick Viscuso, Gary Guissanie, Kelley Dempsey, & Mark Riddle, *NIST Special Publication 800-171 Revision1:ProtectingControlledUnclassified Information in NonfederalSystems and Organizations*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Dec. 2016), *available at* https://doi.org/10.6028/NIST.SP.800-171r1.

[88] Maytech Staff, *supra*, note 62.

[89] HiTrust Staff, *Introduction to the HITRUST CSF*, HITRUST (Dec. 2021), *available at*https://hitrustalliance.net/content/uploads/CSFv9.4_Introduction.pdf.

[90]*Id.*

[91]*Id.*

[92]*Id.*

[93]*Id.*

[94]*Id.*

[95]*Id.*

[96]*Id.*

[97]*Id.*

[98]*Id.*

[99]Angela Fitzpatrick, *HITRUST isShakingThingsUp: Details for the New HITRUST i1 Certification and bC Assessment*, MEDITOLOGY SERVICES (Nov. 22, 2021), *available at*https://www.meditologyservices.com/hitrust-is-shaking-things-up-details-for-the-new-hitrust-i1-certification-and-bc-assessment/#:~:text=The%20HITRUST%20i1%20certification%20incorporates,of%20the%20HIPAA%20Security%20Rule..

[100]*Id.*

HITRUST bC provides a low-level security assurance with only 71 security controls.[101] HITRUST i1 provides a moderate level of security assurance and incorporates the NIST SP 800-171 controls framework and a subset of the HIPAA Security Rule controls.[102]This means that an entity that is HITRUST i1 compliant is likely CMMC 2.0 Level 2 compliant. The HITRUST i1 certification is good for only one year. Entities are evaluated against their implementation of controls. The HITRUST i1 is a certifiable assessment and demands an external assessor firm to evaluate a firm. The HITRUST r2 (formerly known as CSF) certification provides a high level of assurance with a minimum review of 198 controls and up to 2000+ controls. The HITRUST r2 certification is valid for two years, with an interim review at the end of one year. Entities are appraised on security policies, procedures, implementation, measurement, and managed practices.[103] The HITRUST r2 certification is a comprehensive standard that includes CF and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.[104] Given the complexity and number of requirements, a HITRUST r2 compliant firm is probably CMMC 2.0 Level 3 complaint

Compliance Issues with CMMC and the SEC Proposed Changes

Given the SEC's 2022 cyber rule amendments, the question is whether the DoD's CMMC framework is viable. The corporate response revolves around several factors. If the firm is currently a DoD contractor or sub-contractor, then CMMC compliance is critical. The firm's current cyber security status is significant because depending on what cyber security risk management and supply chain management frameworks are currently in place, will determine how the firm will react. For example, if the organization is currently NIST SP 800-171, NIST SP 800-172, or HITRUST 2r (CSF) compliant, there may be only a modicum of work that needs to be accomplished. If the firm is HITRUST 2r compliant, it may be a simple task to discover if their compliance satisfies the DoD CMMC framework.

On the other hand, if the firm is CF or ISO/IEC 27001 compliant, there may be much more work to be done because these security frameworks are neither NIST SP 800-171 nor NIST SP 800-172 comparable. Additional security requirements must necessarily be implemented.The company may have already started implementing the CMMC framework on its own accord and may be well along in its implementation efforts. In this instance, presuming that the entity is well into its implementation, there may not be much work to do. The key to understanding what a company has to do to achieve CMMC compliance, assuming that it wants to attain compliance, is to establish the initial cyber security position of the firm via gap analysis, along with the effort and resources necessary to accomplish CMMC compliance. It should be remembered that a firm could always decide that CMMC compliance is not a goal it wishes to pursue. The company may be content with remaining CF or ISO/IEC 27001 compliant.

Given the SEC's proposed rule changes, the critical issue is whether a firm is a public or private company. If the entity is a closely-held private company, then the SEC cyber rule changes do not apply. What does apply are state cyber breach reporting laws, mainly in those states where the firm is incorporated, is headquartered, or conducts business. For example, suppose the company sells its goods or services in California. In that case, it will be subject to the California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA).[105] The firm could also be subject to the privacy laws in Colorado and Virginia, presuming it does business in these states.[106]

In contrast, a public company, an entity whose stock is publicly traded on a particular stock exchange, such as the New York Stock Exchange (NYSE), would be subject to the SEC's proposed cyber rule changes. The issue facing a public company is whether it currently possesses a cyber security framework and is sufficiently mature to permit the firm to address the proposed rule changes effectively and quickly. If an organization has implemented a cyber framework, the implementation may not be up to the task assigned to the firm by the SEC. This might necessitate substantial effort on the part of the firm to become SEC-compliant. In business, timing is everything. The SEC rule changes will likely increase the firm's compliance complexity layer. The interrelationship between its cyber security framework and the SEC rule changes may not be well understood. There is a possibility for mistakes to be made. Whether the errors are covert or overt depends on the firm's current cyber situation and the quality of board of directors and senior and middle management.

CONCLUSION

In conclusion, there are serious cyber security efforts afoot to combat the multiple variants of cyber-attacks, ransom ware being one such attack. The DoD-supported CMMC framework is a comprehensive methodology to mitigate an attack and assure that companies are adequately protected and that individuals are promptly notified of an attack. The SEC proposed cyber rule changes are another avenue whereby publicly traded firms must inform stockholders about an attack. Although there may be timing issues that have yet to be analyzed and digested, the objective of the CMMC framework, when coupled with the SEC proposed rule changes, is to reduce the effects of cyber-attacks by promoting cyber security awareness and prevention as part of an ongoing business model, just like GAAP accounting is now part of normal business behavior. Cyber-attacks will only decrease when defenses are well understood and established. It is the only way to go.

Donald L. Buresh Biography

Donald L. Buresh earned his Ph.D. in engineering and technology management from North central University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cyber security policy and an M.S. in cyber security concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée at a local fencing club. Dr. Buresh is a member of the Florida Bar.

[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA HIGH TECH. L. J. 1, 39-93 (Oct. 2021), https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
[106] *Id.*

Miscellaneous Considerations

Author Contributions: The author has read and agreed to the published version of the manuscript.
Funding: This research received no external funding.
Institutional Review Board Statement: Not applicable.
Informed Consent Statement: Not applicable.
Conflicts of Interest: The author declares no conflict of interest.
Acknowledgments: Not applicable.
List of Abbreviations:

The following abbreviations are used in this manuscript:

Abbreviation	Description
APT	Advanced Persistent Threats
CCPA	California Consumer Privacy Act
CPRA	California Privacy Rights Act
CF	NIST Cyber security Framework
CMMC	Cyber security Maturity Model Certification
CSF	HITRUST Cyber Security Framework
CUI	Controlled Unclassified Information
DIB-CAC	Defense Industrial Base Cyber security Assessment Center
DoD	Department of Defense
FR	Federal Register
GAAP	Generally Accepted Accounting Principles
HIPAA	Health Insurance Portability and Accountability Act
HITRUST bC	HITRUST Basic, Current-state
HITRUST i1	HITRUST Implemented, 1-year
HITRUST r2	HITRUST Risk-based, 2-year
IEC	International Electro technical Commission
ISO	International Organization for Standardization
NCSL	National Council of State Legislatures
NIST	National Institute of Standards and Technology
NYSE	New York Stock Exchange
POA&M	Plans of Actions & Milestones
RTP	Risk Treatment Plan
SEC	Securities and Exchange Commission
SoA	Statement of Applicability
SSN	Social Security Number
SSP	System Security Plan
XBRL	extensible Business Reporting Language

****